Google Scholar BETA

Web Images Video News Maps more »

symmetric key encrypt secret key Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Search only in Engineering, Computer Science, and Mathematics.
Search in all subject areas.

Scholar All articles - Recent articles Results 1 - 10 of about 19,700 for symmetric key encrypt secr

Encrypted key exchange: password-based protocols secure againstdictionary attacks - all 89 versions »
SM Bellovin, M Merritt - Research in Security and Privacy, 1992. Proceedings., 1992 ..., 1992 - ieeexplore.ieee.org
... The password: a shared secret, often used as a key. Random secret keys (for symmetric cryptosystems). Symmetric (secret-key) encryption of "in f 0" with key R. ...
Cited by 641 - Related Articles - Web Search

A Key-Management Scheme for Distributed Sensor Networks - all 28 versions »
L Eschenauer, VD Gligor - portal.acm.org
... Symmetric key pre-distribution has been used in past ... and to setup a common secret key; however, memory ... Other work on broadcast encryption [4] focuses on key ...
Cited by 304 - Related Articles - Web Search

A concrete security treatment of symmetric encryption - all 16 versions »
M Bellare, A Desai, E Jokipii, P Rogaway - Proceedings of the 38th Annual Symposium on Foundations of ..., 1997 - doi.ieeecs.org
... In the public key setting she can create them her- self given the public key, but in the symmetric key set- ting the encryption key is secret so we must modify ...
Cited by 404 - Related Articles - Web Search - BL Direct

Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and ... - all 71 versions »
SM Bellovin, M Merritt - Proceedings of the 1st ACM conference on Computer and ..., 1993 - portal.acm.org
... Symmetric (secret-key) encryption of"info" with key K. Symmetric (secret-key) decryption of"info" with key K. Digital signature of M with (private) key Sk. ...
Cited by 245 - Related Articles - Web Search

[PS] Secure integration of asymmetric and symmetric encryption schemes - all 5 versions »
E Fujisaki, T Okamoto - Advances in Cryptology—CRYPTO, 1999 - di.ens.fr
... Hybrid Encryption An asymmetric encryption scheme is usually employed only for distributing a secret-key of a symmetric encryption scheme for message encryption ...
Cited by 283 - Related Articles - View as HTML - Web Search - BL Direct

An optimal class of symmetric key generation systems
R Blom - Proc. of the EUROCRYPT 84 workshop on Advances in cryptology . . ., 1985 - portal.acm.org
... optimal class of symmetric key generation systems. ... Authentication Codes and Key Predistribution Schemes ... communication in broadcast encryption schemes, Discrete ...
Cited by 326 - Related Articles - Web Search

Authentication and authenticated key exchanges - all 10 versions »
W Diffie, PC Oorschot, MJ Wiener - Designs, Codes and Cryptography, 1992 - Springer
... the secret key SA corresponding to PA, then she has provided evidence to Bob that she is in fact Alice. Encryption using a symmetric cryptosystem with key K. ...
Cited by 577 - Related Articles - Web Search

Google Scholar BETA

Web Images Video News Maps more »

SKIP key exchange 1776 - 2000 Search

Search only in Engineering, Computer Science, and Mathematics.

Search in all subject areas.

Scholar All articles - Recent articles Results 1 - 10 of about 4,710 for SKIP key exchange. (0.68 se

Securing the commercial Internet - all 5 versions »
A Bhimani - Communications of the ACM, 1996 - portal.acm.org
... Simple Key Exchange for Internet Protocols (SKIP) [4]. SKIP makes use of public-key certificates to exchange long-term symmetric keys between two communicating ...
Cited by 183 - Related Articles - Web Search - BL Direct

Java security: present and near future - all 8 versions »
L Gong, MV JavaSoft - Micro, IEEE, 1997 - ieeexplore.ieee.org
... Page 4. For example, SSL and SKIP support different "flavors," in that the user has a choice of which algorithm to use for key exchange and which to use for ...
Cited by 111 - Related Articles - Web Search - BL Direct

Internet security: firewalls and beyond - all 4 versions »
R Oppliger - Communications of the ACM, 1997 - portal.acm.org
... SDNS Secure Data Network System SHA Secure Hash Algorithm S-HTTP Secure Hypertext Transfer Protocol SKEME Secure Key Exchange Mechanism SKIP Simple Key ...
Cited by 121 - Related Articles - Web Search - BL Direct

New security architectural directions for Java - all 6 versions »
L Gong, C JavaSoft - Compcon'97. Proceedings, IEEE, 1997 - ieeexplore.ieee.org
... One flavor would be to use Diffie-Hellman for key exchange and triple-DES for traffic ... of the JDK toolkit, Java-based implementa- tions of SSL and SKIP may be ...
Cited by 47 - Related Articles - Web Search - BL Direct

The VersaKey Framework: Versatile Group Key Management - all 18 versions »
M Waldvogel, G Caronni, D Sun, N Weiler, B ... - IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 1999 - ieeexplore.ieee.org
... eg, the group key management protocol (GKMP) [13], [14], the simple key-management for Internet protocols (SKIP) [15], the Internet key exchange (IKE) [16 ...
Cited by 240 - Related Articles - Web Search - BL Direct

Secure Multicast
P Pessi - Proc. of Helsinki University of Technology Seminar on ..., 1995 - tml.tkk.fi
... It is intended especially for IP-level datagram based traffic. SKIP uses an alternative version of the Diffie-Hellman (DH) key exchange protocol. ...
Cited by 10 - Related Articles - Cached - Web Search

Secure virtual private networks: the future of data communications - all 3 versions »
E Herscovitz - International Journal of Network Management, 1999 - portal.acm.org
... Other options include the types of algorithms used for encryption—DES/3XDES, RSA, RC4, RC5, IDEA, etc.—and key exchange (IKE, SKIP)—as well as the means ...
Cited by 21 - Related Articles - Web Search - BL Direct

Improvement of Gunther's identity-based key exchange protocol - all 3 versions »
S Saxena - Electronics Letters, 2000 - ieeexplore.ieee.org